IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

Listing of Claims

1-9 (canceled)

10. (currently amended) An information processing device ~~having first storage means and first decoding means for using encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information,~~comprising:

~~the~~ first storage means, for storing an encrypted first key encrypted by a second key, the first storage means comprising:

first ~~mutual authentication~~ authentication means for ~~carrying out mutual authentication with the first decoding means~~ authenticating and generating a temporary key~~,~~;

~~second storage means for storing the second key, second decoding~~ first encrypting/decrypting means for ~~decoding~~ decrypting the encrypted first key with the second key, and ~~encryption means~~ for encrypting the first key with the temporary key~~,~~; and

transmitting means for transmitting the encrypted first key with the temporary key;

~~the first~~ decoding means comprising:

second ~~mutual~~ authentication means for ~~carrying out mutual authentication with~~ authenticating the first storage means and sharing the temporary key with the first storage means; ~~generating a temporary key,~~

receiving means for receiving the encrypted first key with the temporary key from the first storage means; and

~~third~~ second encrypting/decrypting ~~decoding~~ means for ~~decoding~~ decrypting the encrypted first key with the temporary key~~,~~; ~~and~~

wherein the ~~fourth~~ decoding means ~~for decoding~~ decodes the information with the first key obtained by the second encrypting/decrypting means.

11. (currently amended) An information processing method ~~for an information processing device having storage means and decoding means for using encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information,~~ comprising:

a first storage step of storing an encrypted first key encrypted by a second key;

~~the storage means including~~ a first ~~mutual~~ authentication step of ~~carrying out mutual authentication with the decoding means for~~ authenticating the first storage step and generating a temporary key~~;~~;

~~a storage step of storing the second key,~~

a first ~~decoding~~ encrypting/decrypting step of ~~decoding~~ decrypting the encrypted first key with the second key, and ~~an encryption step of~~ encrypting the first key with the temporary key~~;~~;

transmitting the encrypted first key with the temporary key;

a ~~the decoding means including~~ first decoding step that includes a second mutual authentication step of ~~carrying out mutual authentication with~~authenticating the first storage ~~means~~ step and for sharing the ~~generating a~~ temporary key with the first storage step;~~,~~

receiving the encrypted first key with the temporary key;

a second ~~decoding~~ encrypting/decrypting step of ~~decoding~~ decrypting the encrypted first key with the temporary key;~~,~~ and

a second ~~third~~ decoding step of decoding the information with the first key obtained by the second encrypting/decrypting step.

12. (currently amended) A program providing medium for providing a computer-readable program with respect to an information processing device ~~having storage means and decoding means for using encrypted information, an encrypted first key for decoding the information and a second key for decoding the first key so as to decode the information,~~ comprising:

~~the program causing the storage means to execute processing comprising:~~

a first storage step of storing an encrypted first key encrypted by a second key;

a first ~~mutual~~ authentication step of ~~carrying out mutual authentication with the decoding means~~ authenticating and ~~for~~ generating a temporary key;

~~a storage step of storing the second key;~~

a first ~~decoding~~ encrypting/decrypting step of encrypting/decrypting ~~decoding~~ the encrypted first key with the second key~~;~~ and for ~~an encryption step of~~ encrypting the first key with the temporary key;

transmitting the encrypted first key with the temporary key;

the program causing the decoding means to execute processing comprising:

a second ~~mutual~~ authentication step of ~~carrying out mutual authentication~~ authenticating ~~with~~ the first storage step ~~means~~ and for sharing the temporary key with the first storage step ~~generating a temporary key~~;

receiving the encrypted first key with the temporary key from the first storage step;

a second encrypting/decrypting ~~decoding~~ step of ~~decoding~~ decrypting the encrypted first key with the temporary key; and

a third decoding step of decoding the information with the first key obtained by the second encrypting/decrypting step.

13-38 (canceled)

39. (currently amended) An information processing device for processing data ~~decoding and using encrypted information, the device~~ comprising:

permission information generation means for generating permission information of the data or updating the permission information for processing the data ~~information indicating a permission condition for the use of the information~~;

authentication information generation means for generating authentication information of ~~the information indicating~~ the permission ~~condition~~ information; and

storage means for storing the authentication information.

40. (original) The information processing device as claimed in claim 39, wherein the storage means has a tamper-resistant structure.

41. (currently amended) An information processing method for processing data ~~decoding and using encrypted information, the method~~ comprising:

a permission information generation step of generating permission information of the data or updating the permission information for processing the data ~~information indicating a permission condition for the use of the information~~;

an authentication information generation step of generating authentication information of ~~the information indicating~~ the permission ~~condition~~ information; and

a storage step of storing the authentication information.

42. (currently amended) A program providing medium for providing a computer-readable program which causes an information processing device for processing data ~~decoding and using encrypted information to execute processing~~ comprising:

a permission information generation step of generating permission information of the data or updating the permission information for processing the data ~~information indicating a permission condition for the use of the information~~;

an authentication information generation step of generating authentication information of ~~the information indicating~~ the permission ~~condition~~ information; and

a storage step of storing the authentication information.

43. (currently amended) An information processing device for storing information to ~~a loaded~~ an information storage medium ~~and using the information, the device~~ comprising:

interfacing means for interfacing with the information storage medium;

authentication information generation means for generating authentication information of the information ~~related information necessary for the use of~~ as a result of calculating the information;

storage means for storing the authentication information;

verification means for generating another authentication information by the authentication information generating ~~from the related information~~ and verifying coincidence with the authentication information stored by the storage means; and

control means for storing the information to the information storage medium according to the coincidence.

~~mutual authentication means for carrying out mutual authentication with the information storage medium.~~

44. (canceled)

45. (original) The information processing device as claimed in claim 43, further comprising encryption means for encrypting the authentication information.

46. (original) The information processing device as claimed in claim 45, further comprising decoding means for decoding the encrypted authentication information stored by the storage means.

47. (currently amended) An information processing method for an information processing device for storing information to ~~a loaded~~ an information storage medium ~~and using the information~~, the method comprising:

an interfacing step of interfacing with the information storage medium;

an authentication information generation step of generating authentication information of the ~~related~~ information ~~necessary for the use of~~as a result of calculating the information;

a storage step of storing the authentication information;

a verification step of generating another authentication information by the authentication information generation step ~~from the related information~~ and verifying coincidence with the authentication information stored at the storage step; and

a controlling step of controlling storage of the information to the information storage medium according to the coincidence.

~~a mutual authentication step of carrying out mutual authentication with the information storage medium.~~

48. (currently amended) A program providing medium for providing a computer-readable program which causes an information processing device for storing information to ~~a loaded~~ an information storage medium ~~and using the information, to execute processing~~ comprising:

an interfacing step of interfacing with the information storage medium;

an authentication information generation step of generating authentication information of ~~related information necessary for the use of~~ the information as a result of calculating the information;

a storage step of storing the authentication information;

a verification step of generating another authentication information by the authentication information generation step ~~from the related information~~ and verifying coincidence with the authentication information stored at the storage step; and

a controlling step of controlling storage of the information to the information storage medium according to the coincidence.

~~a mutual authentication step of carrying out mutual authentication with the information storage medium.~~

49. (currently amended) An information storage medium for storing encrypted information ~~and being loaded~~ on an information processing device, the medium comprising:

interfacing means for interfacing with the information storage medium;

authentication information generation means for generating authentication information of ~~related information necessary for the use of~~ the information as a result of calculating the information;

storage means for storing the authentication information;

verification means for generating another authentication information by the authentication information generating ~~from the related information~~ and verifying coincidence with the authentication information stored by the storage means; and

control means for storing the information to the information storage medium according to the coincidence.

~~mutual authentication means for carrying out mutual authentication with the information processing device.~~

50. (original) The information storage medium as claimed in claim 49, further comprising encryption means for encrypting the authentication information.

51. (original) The information storage medium as claimed in claim 49, further comprising decoding means for decoding the encrypted authentication information stored in the storage means.

52-58 (canceled)

59. (currently amended) An information processing device for processing data stored in an external storage medium ~~storing predetermined information to an external storage medium loaded therein, and for decoding encrypted information and using the decoded information, the device~~ comprising:

interfacing means for communicating with the external storage medium;

~~mutual authentication~~ authenticating means for ~~carrying out mutual authentication~~ authenticating ~~with~~ the external storage medium ~~loaded therein;~~ and sharing a predetermined key with the external storage medium;

encrypting ~~encryption~~ means for encrypting the data ~~predetermined information~~ with the ~~a~~ predetermined key; and

transmitting the encrypted data via the interfacing means to the external storage medium.

60. (original) The information processing device as claimed in claim 59, wherein the predetermined key is a public key of a management device managing the information

processing device.

61. (currently amended) An information processing method for an information processing device for processing data stored in an external storage medium ~~storing predetermined information to an external storage medium loaded therein, and for decoding encrypted information and using the decoded information, the method~~ comprising:

a communicating step of communicating with the external storage medium;

an authenticating ~~a mutual authentication~~ step of ~~carrying out mutual authentication~~ authenticating ~~with~~ the external storage medium ~~loaded therein;~~ and sharing a predetermined key with the external storage medium;

an encryption step of encrypting the data ~~predetermined information~~ with ~~a~~ the predetermined key; and

a transmitting step of transmitting the encrypted data via the communicating step to the external storage medium.

62. (currently amended) A program providing medium for providing a computer-readable program which causes an information processing device for processing data stored in an external storage medium ~~storing predetermined information to an external storage medium loaded therein and for decoding encrypted information and using the decoded information, to execute processing~~ comprising:

a communication step of communicating with the external storage medium;

an authentication ~~a mutual authentication~~ step of ~~carrying out mutual authentication with~~ authenticating the external storage medium ~~loaded therein;~~ and sharing a predetermined key with the external storage medium;

an encryption step of encrypting the data ~~predetermined information~~ with ~~a~~ the predetermined key;

a transmission step of transmitting the encrypted data via the communication step to the external storage medium.

63- 67 (canceled)

68. (new) The information processing device according to claim 10, wherein the first storage means is tamper-resistant.

69. (new) The information processing device according to claim 39, wherein the authentication information generated and stored in the storage means is compared with authentication information when the data is processed.

70. (new) The information processing device according to claim 39, wherein the data is a content and permission information is a license of the content.

71. (new) The information processing device according to claim 39, wherein the authentication information generation means calculates a hash of the permission information.